Dr.WEB®

CureIt!®

Defend what you create

# User Manual

**© 2015 Doctor Web. All rights reserved.**

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

TRADEMARKS
Dr.Web, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

**Dr.Web® CureIt!®**
**User Manual**
**27.07.2015**

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

# Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

**We thank all our customers for their support and devotion to the Dr.Web products!**

# Table of Contents


**Document Conventions** 5

**Dr.Web CureIt!** 6

- **System Requirements** 7
- **Testing Anti-virus** 8
- **Detection Methods** 9
- **Sending Statistics** 10

**Quick Start** 11

- **Dr.Web CureIt! Update** 11
- **Express Scan** 12
- **Quarantine Manager** 15

**Advanced Options** 17

- **Running Custom Scan** 17
- **Configuring Threat Neutralization** 19
- **Configuring Scanning** 20
  - Main Tab 21
  - Actions Tab 22
  - Exclusions Tab 23
  - Log Tab 24
- **Launching From Command Line** 25
  - Command Line Parameters 26

**Technical Support** 29

# Document Conventions

This guide utilizes the following content conventions and signs (see Table 1).

**Table 1. Document Conventions and Signs**

| Convention | Description |
|---|---|
| **Bold** | Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide. |
| **Green and bold** | Names of **Doctor Web** products and components. |
| Green and underlined | Hyperlinks to topics and web pages. |
| `Monospace` | Code examples, input to the command line and application output. |
| *Italic* | Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values.<br>In addition, it may indicate a term in position of a definition. |
| CAPITAL LETTERS | Names of keys and key sequences. |
| Plus sign ('+') | Indicates a combination of keys. For example, ALT+F1 means to hold down the ALT key while pressing the F1 key. |
| Exclamation mark | A warning about potential errors or any other important comment. |

# Dr.Web CureIt!

**Dr.Web® CureIt!®** is an anti-virus scanner based on **Dr.Web Scanning Engine**, the standard virus scanning engine of **Dr.Web products**. Although **Dr.Web CureIt!** has limited performance capabilities in comparison with **Dr.Web Anti-virus for Windows** (no resident monitor, no command line scanner, no updating utility, etc.), it is nevertheless able to effectively scan the system and perform necessary actions for detected threats.

**Dr.Web CureIt!** detects and neutralizes the following types of malicious programs:

- Worms
- Viruses
- Trojans
- Rootkits
- Spyware
- Dialers
- Adware
- Hacktools
- Jokes
- Riskware

**Dr.Web CureIt!** is the ideal solution for situations when installation of an anti-virus is impossible due to virus activity or some other reason, because it does not require installation, operates under Microsoft® Windows® and Microsoft® Windows Server® operating systems for 32 or 64-bit platforms (from Microsoft Windows XP and to Microsoft Windows 8.1) and is constantly supplemented with the latest **Dr.Web virus databases** to ensure its effectiveness against all virus threats and other malicious programs. It also automatically defines the language used by your operating system. If your language is not supported, then **Dr.Web CureIt!** will use English by default.

**Dr.Web CureIt!** sends general information on your computer and its state of information security to **Doctor Web**. When using
**Dr.Web CureIt!** (Commerce Edition), statistics gathering is optional.

It is recommended to run **Dr.Web CureIt!** under an account with administrative privileges. Otherwise, all folders and files that are not accessible to unprivileged user including system folder are not scanned.

# System Requirements

To use **Dr.Web CureIt!**, your computer should meet the following requirements:

| Specification | Requirement |
|---|---|
| OS | For 32-bit platforms:<br>• Windows XP with Service Pack 2 or 3<br>• Windows Vista<br>• Windows 7<br>• Windows 8<br>• Windows 8.1<br>• Windows 10<br>• Windows Server 2003 SP1<br>• Windows Server 2008<br>For 64-bit platforms:<br>• Windows Vista<br>• Windows 7<br>• Windows 8<br>• Windows 8.1<br>• Windows 10<br>• Windows Server 2008<br>• Windows Server 2008 R2<br>• Windows Server 2012<br>• Windows Server 2012 R2 |
| Hard disk space | 160 MB of disk space. |
| Free RAM | Minimum 360 MB of RAM. |
| CPU | i686 compatible. |

# Testing Anti-virus

The EICAR(European Institute for Computer Anti-Virus Research) Test File helps testing performance of anti-virus programs that detect viruses using signatures.

For this purpose, most of the anti-virus software vendors generally use a standard test.com program. This program was designed specially so that users could test reaction of newly-installed anti-virus tools to detection of viruses without compromising security of their computers. Although the test.com program is not actually a virus, it is treated by the majority of anti-viruses as if it were a virus. On detection of this "virus", **Dr.Web CureIt!** reports the following: `EICAR Test File (Not a Virus!)`. Other anti-virus tools alert users in a similar way.

The test.com program is a 68-byte COM-file that prints the following line on the console when executed: EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

The test.com file contains the following character string only:

**X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H***

To create your own test file with the "virus", you may create a new file with this line and save it with as test.com.

# Detection Methods

The **Doctor Web** anti-virus solutions use several malicious software detection methods simultaneously, and that allows them to perform thorough checks on suspicious files and control software behavior.

## Detection Methods

### Signature analysis

The scans begin with signature analysis which is performed by comparison of file code segments to the known virus signatures. A *signature* is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, the **Dr.Web** anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. The **Dr.Web virus databases** are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

### Origins Tracing™

On completion of signature analysis, **Dr.Web** uses the unique **Origins Tracing** method to detect new and modified viruses which use the known infection mechanisms. Thus, **Dr.Web** users are protected against such threats as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the **Origins Tracing** mechanism allows to considerably reduce the number of false triggering of the heuristics analyzer. Objects detected using the **Origins Tracing** algorithm are indicated with the `.Origin` extension added to their names.

### Execution emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses, when the search against checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an *emulator* – a programming model of the processor and runtime environment. The emulator operates with protected memory area (*emulation buffer*), in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

### Heuristic analysis

The detection method used by the heuristics analyzer is based on certain knowledge (*heuristics*) about certain features (attributes) than might be typical for the virus code itself, and vice versa, that are extremely rare in viruses. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if the corresponding attribute is indicative of a malicious code or negative if the attribute is uncharacteristic of a computer threat. Depending on the sum weight of a file, the heuristics analyzer calculates the probability of unknown virus infection. If the threshold is exceeded, the heuristic analyzer generates the conclusion that the analyzed object is probably infected with an unknown virus.

The heuristics analyzer also uses the **FLY-CODE™** technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of malicious objects in files compressed not only by packagers **Dr.Web** is aware of, but by also new, previously unexplored programs. While checking packed objects, **Dr.Web** anti-virus solutions also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed

with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristics analyzer may commit type I or type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristics analyzer are treated as "suspicious ".

While performing any of the abovementioned checks, the **Dr.Web** anti-virus solutions use the most recent information about known malicious software. As soon as experts of **Doctor Web Virus Laboratory** discover new threats, the update for virus signatures, behavior characteristics and attributes is issued. In some cases updates can be issued several times per hour.

## Sending Statistics

In order to provide analysis of information security threats and overall viral situation around the globe as well as to ensure continuous development and improvement of **Dr.Web products**, **Dr.Web CureIt!** collects impersonal statistics while it scans and cures your system. This statistics contain only the following general information:

- CPU details including processor name, technical description, current and maximum speed, number of processor cores, and number of logical processors.
- RAM details including amount of physical and virtual memory both total and available at scanning.
- Operating system parameters including its name, version, build number, installed service packs, operation mode, type of account (user or administrative), and locale settings.
- Information on installed anti-virus, anti-spy, and firewall software.
- Information on each detected threat including its name and type, the name and type of infected object, and hash of the infected file when necessary.
- Scan summary including scanning time, number of scanned files and objects, number of suspicious objects, and number of detected threats per type.
- Summary on applied actions including number of unmodified objects as well as number of cured, deleted, moved, renamed, and ignored objects.

The privacy statement from **Doctor Web** is available on the on the official website at http://company.drweb.com/policy/.

If you want to participate in this improvement program, then select the appropriate option when running **Dr.Web CureIt!**.

# Quick Start

**Dr.Web CureIt!** allows you to run anti-virus scans of boot sectors, random access memory (RAM) and both separate files and objects enclosed within complex objects(archives, e-mail attachments, installation packages).

---

**Dr.Web CureIt!** does not check archived files by default. You can enable scanning of archived files in **Dr.Web CureIt!** settings.

---

**Dr.Web CureIt!** uses all detection methods to find viruses and other malicious software and just informs you when a malicious object is found. Information on all infected or suspicious objects displays in the table where you can manually select a necessary action.

The default settings are optimal for most cases. However, if necessary, you can modify actions suggested upon threat detection by using **Dr.Web CureIt!** settings window. Please note that you can set custom action for each detected threat after scan is completed, but common reaction for a particular threat type should be configured beforehand.

**To change interface language**

Click the **Language** icon on the toolbar, and then select the necessary option.

# Dr.Web CureIt! Update

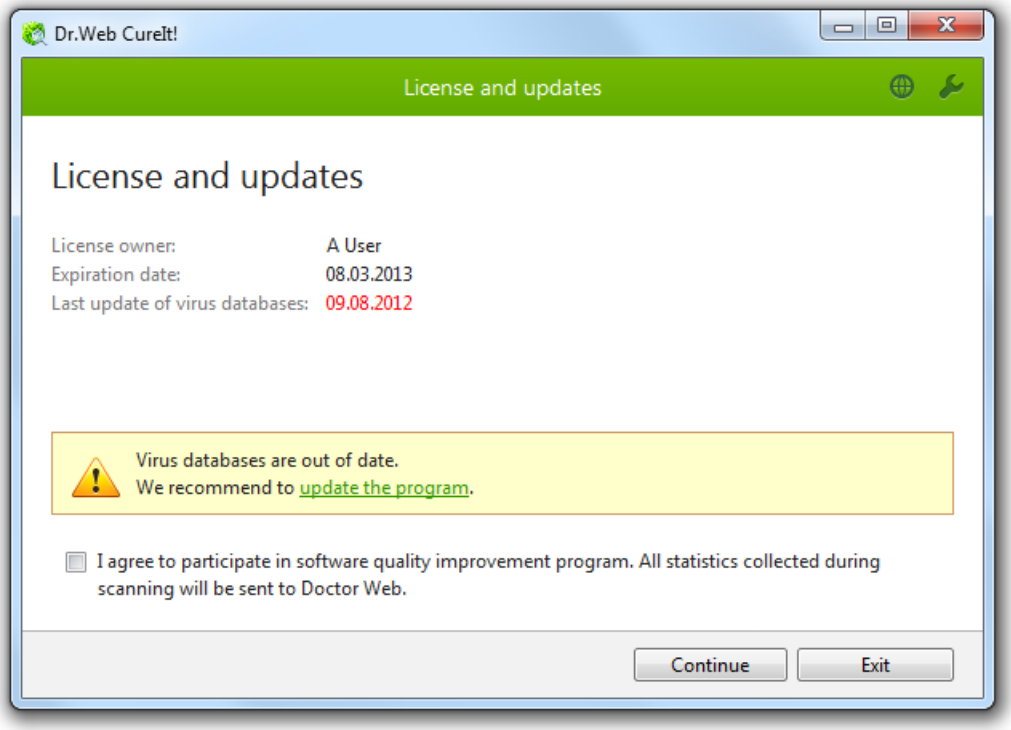
**Dr.Web CureIt!** does not include an updating module, therefore it remains fully efficient only until the next database update (which occurs approximately every hour). After that, to ensure the ultimate anti-virus operation efficiency, the latest version of **Dr.Web CureIt!** should be downloaded again.

The latest **Dr.Web CureIt!** version is always available for download from your personal page on the **official Doctor Web website**. Once you download the program, it acts as a very effective scanner with the latest databases and the most advanced virus detection engine.

**To download latest Dr.Web CureIt!**

1. Run **Dr.Web CureIt!**.
2. When an update is necessary, the first window **License and updates** displays a notification. To update **Dr.Web CureIt!**, click **update the program** in the notification area.

This opens your personal page on the **official Doctor Web website** with the default Internet browser, where you can download the latest version of the **Dr.Web CureIt!** provided that you license has not expired, or renew you license


Dr.Web CureIt!
License and updates
License and updates
License owner: A User
Expiration date: 08.03.2013
Last update of virus databases: 09.08.2012
Virus databases are out of date.
We recommend to update the program.
I agree to participate in software quality improvement program. All statistics collected during scanning will be sent to Doctor Web.
Continue
Exit

## Express Scan

**Dr.Web CureIt!** provides a pre-installed template for anti-virus scanning of the most vulnerable objects of your operating system.

In this mode the following objects are scanned:

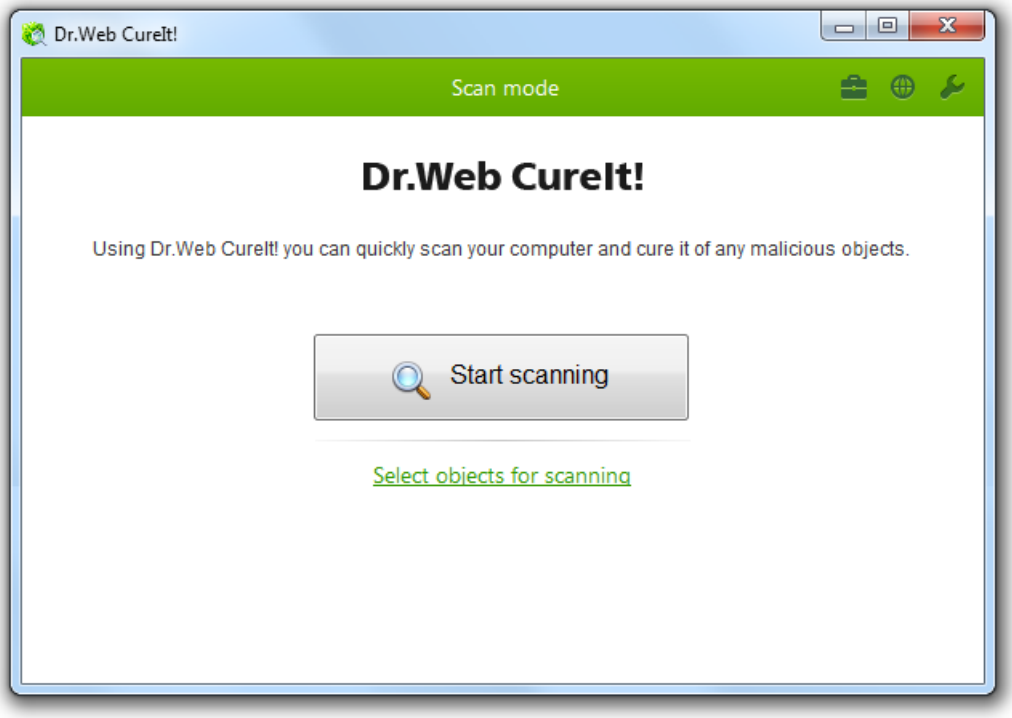
- Random access memory
- Boot sectors of all disks
- Boot disk root folder
- Disk root storing the Windows installation folder
- Windows system folder
- User documents folder ("My documents")
- System temporary files
- User temporary files

If scanning process is running under administrative privileges, then in this mode **Scanner** also checks if rootkits are present in the system.

If a more flexible configuration of an anti-virus scanning is required, you can perform a custom scan.

**To run express scans**

1. Run **Dr.Web CureIt!**.
2. In the **License and updates** window, read the conditions of statistics gathering. If you want to participate in this improvement program, then select the appropriate checkbox. Click **Continue**.
3. In the **Scan mode** window, click **Start scanning**.

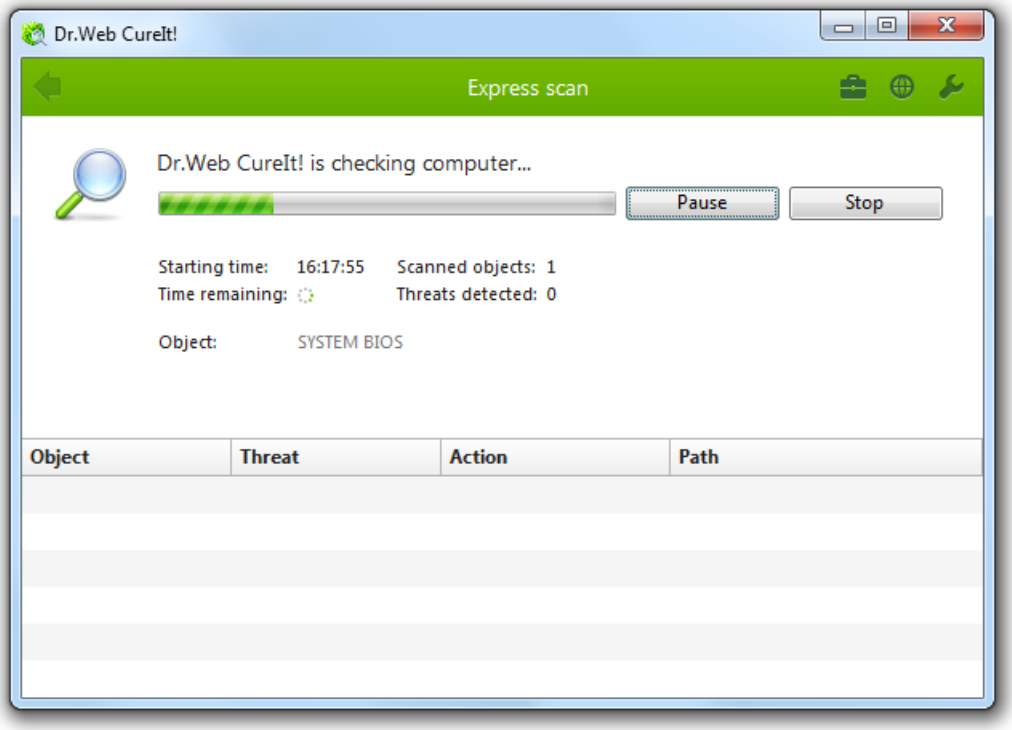

Dr.Web CureIt!
Scan mode
Dr.Web CureIt!
Using Dr.Web CureIt! you can quickly scan your computer and cure it of any malicious objects.
Start scanning
Select objects for scanning

4. During scanning, **Dr.Web CureIt!** displays general information on its progress and lists detected threats.

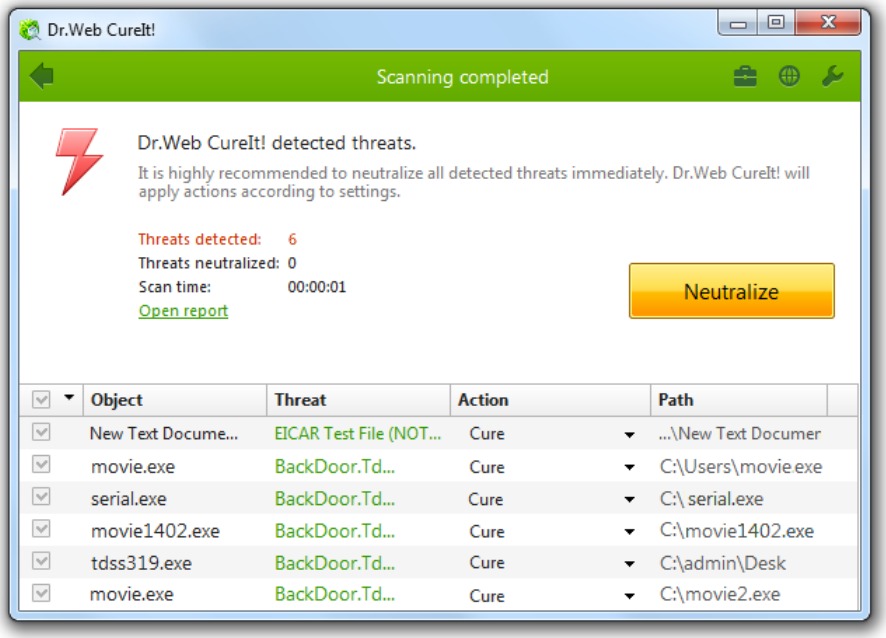
   To manage scanning process, use the following options:

   - To suspend scanning, click **Pause**.
   - To continue with the scanning, click **Resume**.
   - To terminate scanning, click **Stop**.

   The **Pause** button is not available while processes and RAM are being scanned.




5. Once scanning completes, **Dr.Web CureIt!** displays detailed information on detected threats. Review scan results. If necessary, you can also review the scanning log by clicking **Open report**.




6. If scanning reveals viruses or other threats, you need to secure your system by neutralizing them. To apply predefined actions to all detected threats at once, click **Neutralize**. If necessary, you can select custom actions for particular threats.

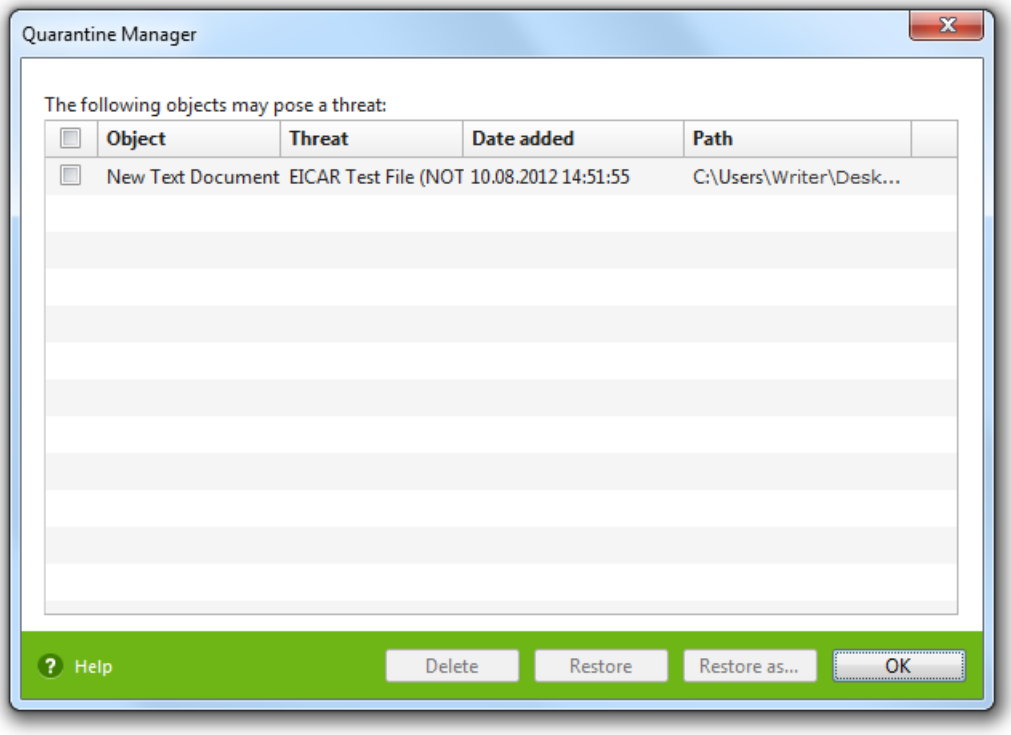
# Quarantine Manager

The **Quarantine** component of **Dr.Web CureIt!** serves for isolation of files that are suspected to be malicious. **Quarantine** also stores backup copies of files processed by **Dr.Web CureIt!**.

**Quarantine** is stored in folder %USERPROFILE%\Doctor Web\DrWeb CureIt Quarantine. Infected objects are moved to the folder, and then the quarantined files located on hard drives are encrypted.

**To open Quarantine Manager**

In the **Dr.Web CureIt!** window, click **Preferences** in the toolbar, and then select **Quarantine Manager**.




The central table lists the following information on quarantined objects that are available to you:

- **Object** – name of the quarantined object
- **Threat** – malware class of the object, which is assigned by **Dr.Web CureIt!** when the object is quarantined
- **Date added** – the date and time when the object was moved to **Quarantine**
- **Path** – full path to the object before it was quarantined

**Quarantine** displays objects which can be accessed by your user account.

To view hidden objects, run **Dr.Web CureIt!** under an administrative account.

**To manage quarantined objects**

1. Select checkboxes for one or more objects that you want to manage.
2. Click one of the following buttons to apply the necessary action:

| Button | Description |
|---|---|
| Restore | Removes the selected objects from the quarantine and restores them to their original location(the folder where the object had resided before it was moved to the quarantine).<br>Use this option only when you are sure that the selected objects are not harmful. |
| Restore to | Removes the selected objects from the quarantine and restores them to selected location.<br>Use this option only when you are sure that the selected objects are not harmful. |
| Delete | Deletes the selected objects from the quarantine and from the system. |

# Advanced Options

For most cases, express scanning is enough to cure your computer from infections and malicious programs. In rare cases when subtle tuning is necessary, use the following options:

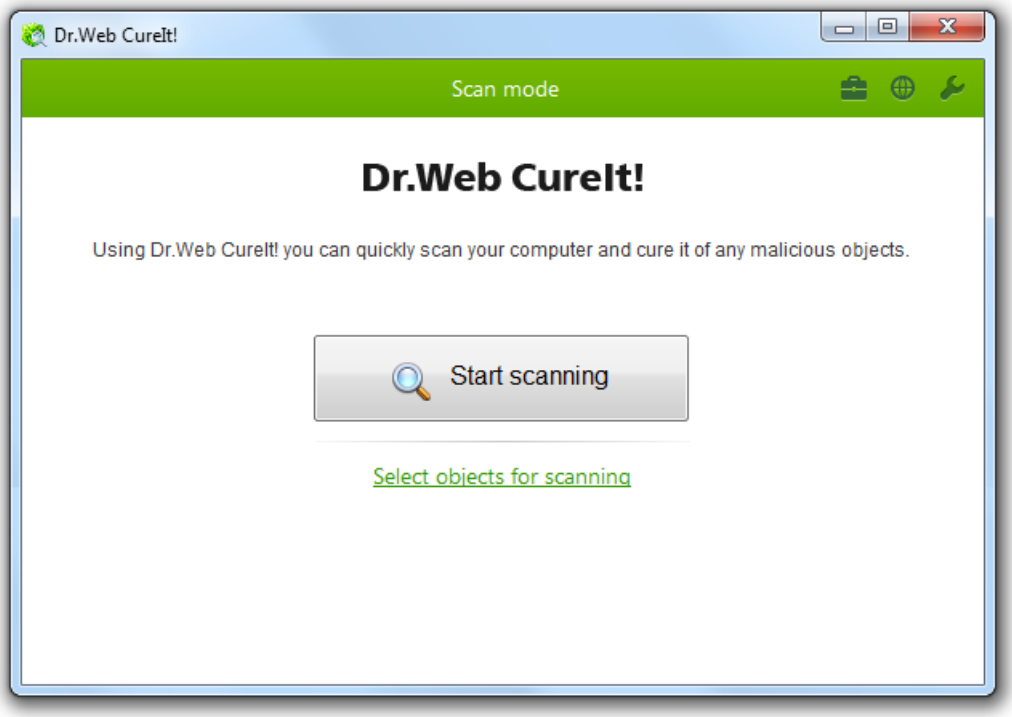
- Perform custom scans, which allows you to select particular operating system objects or files and folders to scan.
- Select custom actions to apply to detected threats.
- Configure general settings of anti-virus scanning.
- Run **Dr.Web CureIt!** from command line using various parameters.

## Running Custom Scan

Apart from the pre-installed scanning template that helps running an express scan of the most vulnerable objects of the operating system, **Dr.Web CureIt!** also provides you with custom scan mode that allows configuring scanning in accordance with your particular needs.

This mode allows you to select objects for scanning: any folders and files, and such objects as random access memory, boot sectors, etc.

You can select a scan type in the **Scan mode** window after launching **Dr.Web CureIt!**.

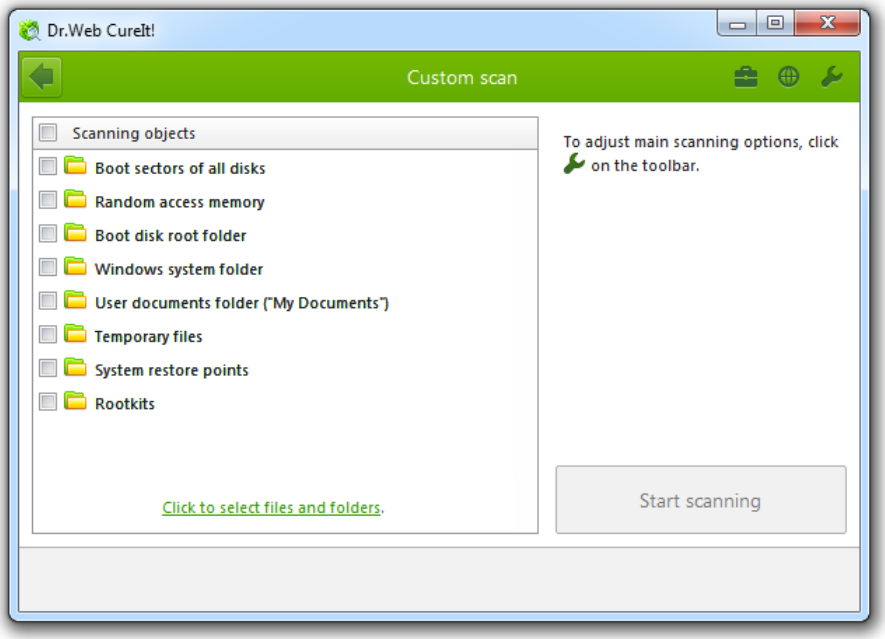

Dr.Web CureIt!
Scan mode
Dr.Web CureIt!
Using Dr.Web CureIt! you can quickly scan your computer and cure it of any malicious objects.
Start scanning
Select objects for scanning

**To run custom scans**

1. Run **Dr.Web CureIt!**.
2. In the **License and updates** window, read the conditions of statistics gathering. If you want to participate in this improvement program, then select the appropriate checkbox. Click **Continue**.
3. In the scan type selection window, click **Select objects for scanning**.

4. The table in the center of this windows lists objects for scanning. You can add files and folders to check for viruses. For this, click the link at the bottom of the table, and then select objects for scanning in the **Browse** window.

   To check all listed objects for viruses, select the **Scanning objects** checkbox in the table heading.

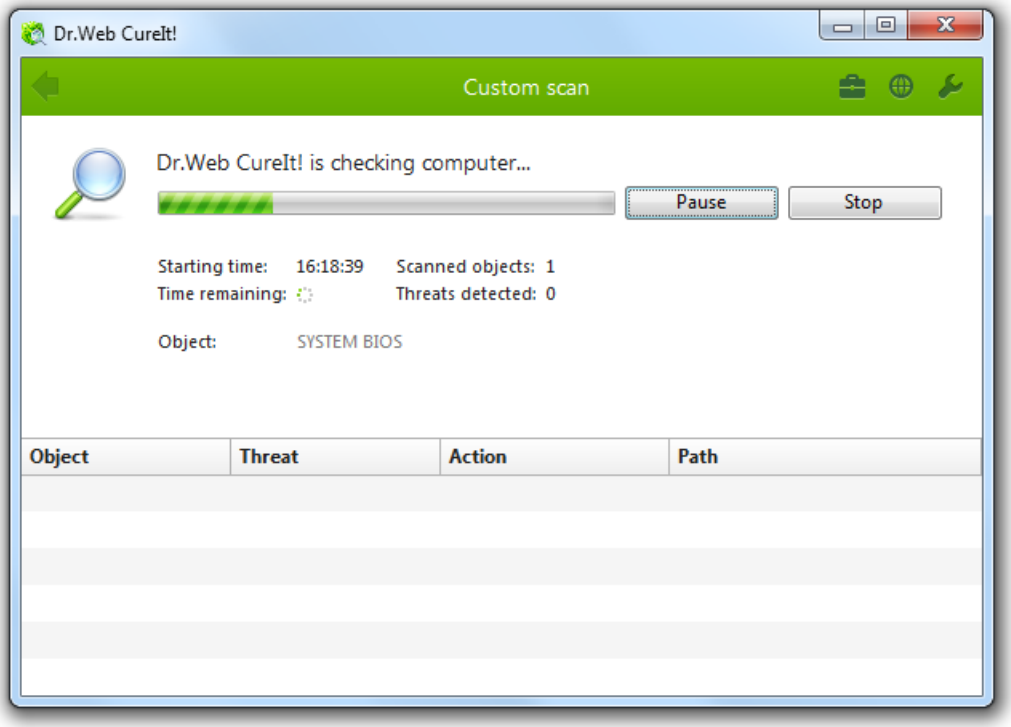



5. If necessary, configure **Dr.Web CureIt!** settings before starting the scan. To do this, click **Preferences** on the toolbar.
6. Click **Start scanning**.
7. During scanning, **Dr.Web CureIt!** displays general information on its progress and lists detected threats.

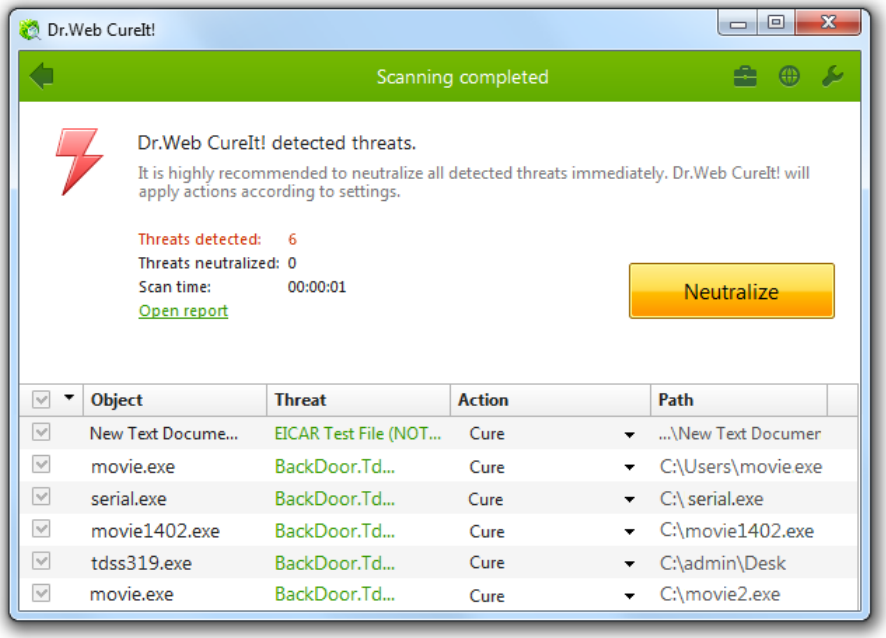
   To manage scanning process, use the following options:

   - To suspend scanning, click **Pause**.
   - To continue with the scanning, click **Resume**.
   - To terminate scanning, click **Stop**.

The **Pause** button is not available while processes and RAM are being scanned.




8. Once scanning completes, **Dr.Web CureIt!** displays detailed information on detected threats. Review scan results. If necessary, you can also review the scanning log by clicking **Open report**.




9. If scanning reveals viruses or other threats, you need to secure your system by neutralizing them. To apply predefined actions to all detected threats at once, click **Neutralize**. If necessary, you can select custom actions for particular threats.

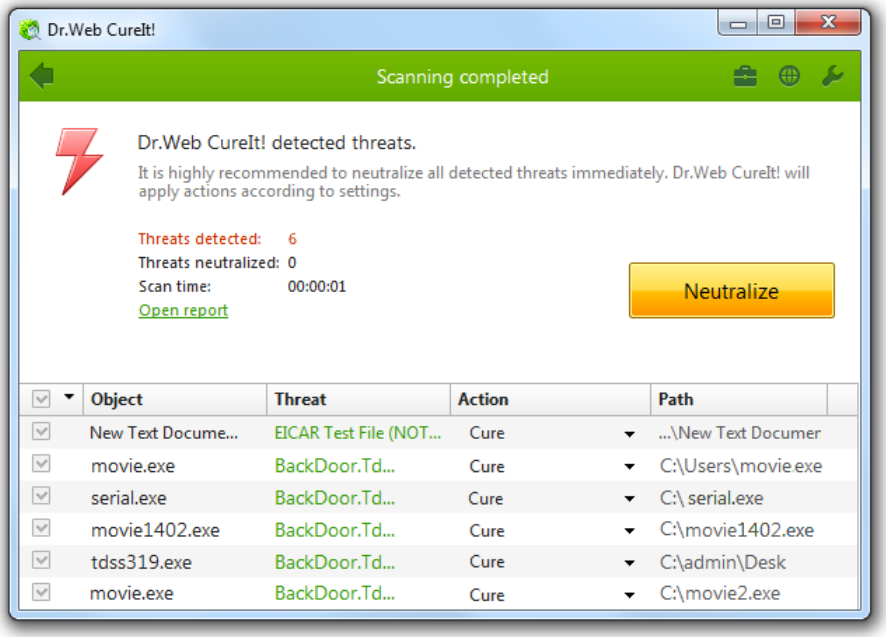
## Configuring Threat Neutralization

By default, if known viruses or computer threats of other types are detected during scanning, **Dr.Web CureIt!** informs you about them. You can neutralize all detected threats at once by clicking

**Neutralize**. In this case **Dr.Web CureIt!** applies the most effective actions in accordance with its configuration and threat type. When necessary, you can apply actions separately or change default action for particular threats.

Threats to your security can be neutralized either by restoring the original state of each infected objects (*curing*), or, when curing is impossible, by removing the infected object completely from your operating system (*deleting*).

By clicking **Neutralize** you apply actions to the objects selected in the table. **Dr.Web CureIt!** selects all objects by default once scanning completes. When necessary, you can customize selection by using checkboxes next to object names or threat categories from the drop-down menu in the table header.




**To select an action**

1. Where necessary, select a custom action from the drop-down list in the **Action** field. By default, **Dr.Web CureIt!** selects a recommended action for the type of detected threat.
2. Click **Neutralize**. **Dr.Web CureIt!** applies selected actions to all detected threats.

Suspicious objects are moved to the quarantine folder and should be sent for analysis to the **Doctor Web Virus Laboratory**.

There are some limitations:

- For suspicious objects curing is impossible.
- For objects which are not files (boot sectors) moving and deletion is impossible.
- For files inside archives, installation packages or attachments, no actions are possible.

The detailed report on **Dr.Web CureIt!** operation is stored in the CureIt.log file that is located in folder %USERPROFILE%\Doctor Web. It is recommended to analyze the log file periodically.

## Configuring Scanning

The default settings are optimal for most uses. Do not change them unnecessarily.

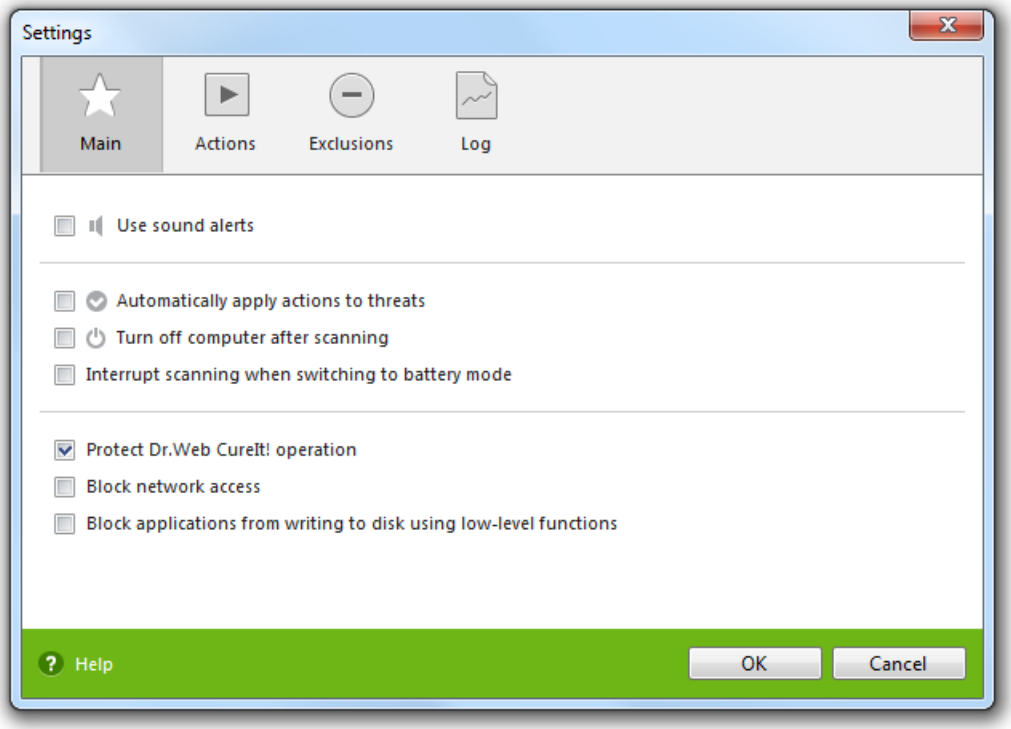
**To configure Dr.Web CureIt!**

1. If **Dr.Web CureIt!** is not running, start the program. This opens the **Dr.Web CureIt!** window.
2. Click the **Preferences** icon on the toolbar, and then select **Settings**. This opens a window opens that contains the following tabs:
   - The Main tab, where you can configure general parameters of **Dr.Web CureIt!** operation.
   - The Actions tab, where you can configure reaction of the **Dr.Web CureIt!** on detection of infected or suspicious files and archives or other malicious objects.
   - The Exclusions tab, where you can specify files and folders to be excluded from scanning.
   - The Log tab, where you can set logging options for **Dr.Web CureIt!**.
3. Configure options as necessary. To get information on options in the tab, click **Help**.
4. After editing, click **OK** to save the changes or **Cancel** to cancel them.

Changes in the settings of **Dr.Web CureIt!** are retained only in the current program session. New session resets program settings to default values.

## Main Tab

On this tab you can set general parameters of **Dr.Web CureIt!** operation.



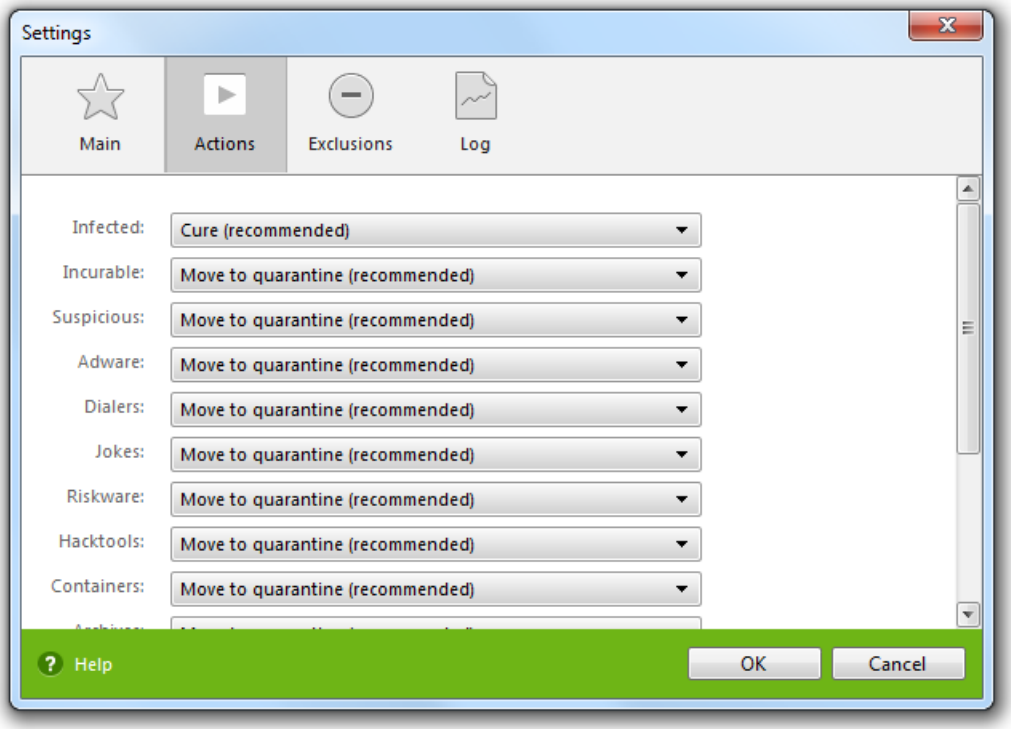

You can enable sound notifications on particular events, set **Dr.Web CureIt!** to apply recommended actions to detected threats automatically, and configure **Dr.Web CureIt!** interaction with the operating system.

On this page, you can also specify self-protection parameters and disable miscellaneous operations that may compromise security of your computer.

It is recommended to run **Dr.Web CureIt!** under an account with administrative privileges. Otherwise, all folders and files that are not accessible to unprivileged user including system folder are not scanned.

# Actions Tab

**Dr.Web CureIt!** just informs you on detection of a malicious object and prompts to neutralize threats by applying suitable actions. These actions are suggested in accordance with the settings on this tab.




The best action for curable threats (e.g. files infected with known viruses) is curing, since it allows to restore the infected file completely. It is recommended to move other threats to quarantine for further analysis in order to prevent loss of potentially valuable data. You can select one of the following actions:

| Action | Description |
|---|---|
| Cure | (Available for known viruses only except Trojan programs that are deleted on detection.)<br>Instructs **Dr.Web CureIt!** to try to restore the original state of an object before infection. If the object is incurable, or the attempt of curing fails, the action set for incurable viruses is applied.<br>This is the only action available for boot sectors. At the same time, this is action is not applicable to files within complex objects(archives, e-mail attachments, file containers). |
| Move to quarantine | Instructs **Dr.Web CureIt!** to move the object to a specific quarantine folder. By default, the quarantined files are located in the %USERPROFILE%\Doctor Web\DrWeb CureIt Quarantine\ hidden folder that becomes accessible once scanning completes.<br>This action is impossible for boot sectors. No action is performed on malicious objects for which you selected this action, if they are detected in a boot sector. |
| Delete | Instructs **Dr.Web CureIt!** to delete the object.<br>This action is impossible for boot sectors. No action is performed on malicious objects for which you selected this action, if they are detected in a boot sector. |
| Ignore | (Available for potentially dangerous files only which includes adware, dialers, jokes, hacktools and riskware.)<br>Instructs **Dr.Web CureIt!** to skip the object without performing any action or displaying a notification. |

Threats within complex objects(archives, e-mail attachments, file containers) cannot be processed individually. For such threats,
**Dr.Web CureIt!** applies an action selected for this type of a complex object and by default implies moving the complex object to the quarantine.

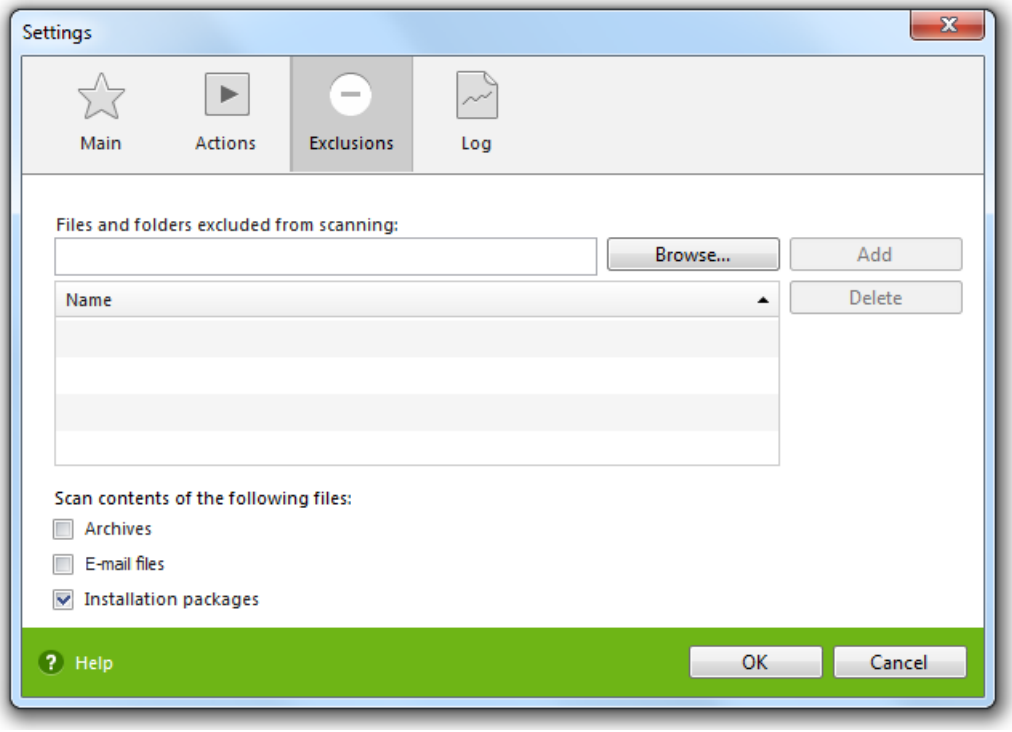
To cure some infected files it is necessary to reboot Windows. You can choose one of the following:

- **Restart computer automatically**. It can lead to loss of unsaved data.
- **Prompt restart**.

## Exclusions Tab

On this tab, you can specify files and folders that should be excluded from scanning and determine whether to scan contents of archives, email files, and installation packages.

Scanning of emails is not allowed by license agreement of the
**Dr.Web CureIt!** (Free Edition). Use **Dr.Web CureIt!** (Commerce Edition) or other **Dr.Web products** to check contents of email files.




# Excluded Files List

Here you can list names or masks for the files to be excluded from scanning. All files with the names which match the name or mask specified will be excluded from scanning (this option is appropriate for temporary files, swap files, etc).

**To configure excluded files list**

Do one of the following:

- To add a file to the list, either enter the full path to the file or click **Browse** and select the file, and then click **Add**. The file will be added to the list. You can also use masks. ‣ Details

A mask denotes the common part of object names, at that:

- The '*' character replaces any, possibly empty, sequence of characters
- The '?' character replaces any character (one)
- Other mask characters do not replace anything and mean that the name must contain this particular character in this place

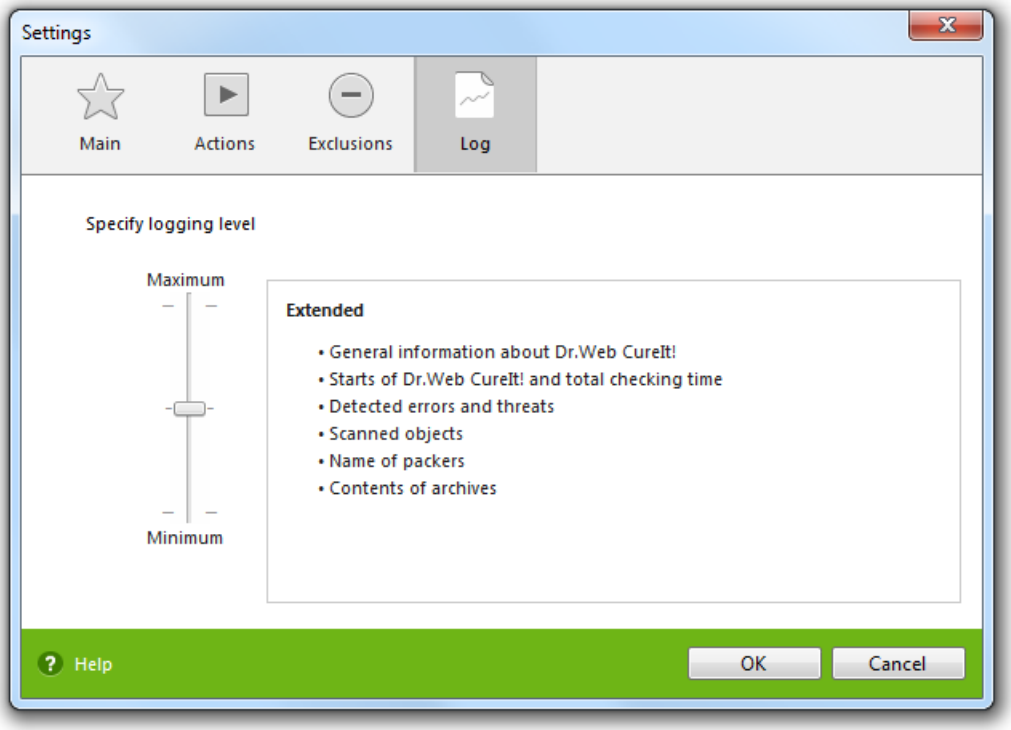
Examples:

- **Report*.doc** defines all Microsoft Word documents which names start with the word "Report" (**Report**February**.doc**, **Report**121209**.doc** etc).
- ***.exe** defines all executable files. i.e. that have the EXE extension (setup**.exe**, iTunes**.exe** etc).
- **photo????09.jpg** defines all JPG images which names start with the word "photo", end with "09" and contain exact number of 4 other characters in the middle (**photo**1212**09.jpg**, **photo**Jude**09.jpg**, **photo**----**09.jpg** etc).

- To remove a file from the list, select it and click **Delete**. The file will be checked on the next scan.

## Log Tab

In the **Log** page you can set up the parameters of the log file.




The **Dr.Web CureIt!** log is stored in the CureIt.log, file that is located in folder %USERPROFILE%\Doctor Web and includes the following information:

| Log Mode | Description |
|---|---|
| Standard | In this mode, **Dr.Web CureIt!** logs the following most important actions only:<br>• Time of **Dr.Web CureIt!** starts and stops<br>• Detected errors and threats |
| Extended | In this mode, **Dr.Web CureIt!** logs the most important actions and the following additional data: |

| Log Mode | Description |
|---|---|
| | • Names of scanned objects<br>• Names of packers<br>• Contents of scanned archives |
| Debugging | In this mode, **Dr.Web CureIt!** logs all details on its activity. This may result in considerable log growth.<br>It is recommended to use this mode only when errors occur or by request of **Doctor Web Technical Support.** |

## Launching From Command Line

You can run **Dr.Web CureIt!** in the command line mode which allows to specify settings of the current scanning session and the list of objects for scanning as additional parameters.

The launching command syntax is as follows:
[<*path_to_program*>][*CureIt!-file_name*] [<*objects*>] [<*switches*>]

The list of objects to be scanned can be left empty or contain several paths separated by blanks. If no path to the objects is specified, **Dr.Web CureIt!** searches for the objects in the **Dr.Web CureIt!** directory.

The most commonly used examples of specifying the objects for scanning are given below:

- **/FAST** perform an express scan of the system.
- **/FULL** perform a full scan of all hard drives and removable data carriers (including boot sectors).
- **/LITE** perform a basic scan of random access memory and boot sectors of all disks. This mode also allows to detect rootkits.

Switches are command line parameters that specify program settings. If no switches are defined, scanning is performed with the settings specified earlier (or with the default settings if you have not changed them). Each switch begins with a forward slash (**/**) character and is separated with a blank from other switches. If a parameter contains a blank space, you have to put quotation marks around it. For example:

- 636frs47.exe /tm-
- 45hlke49.exe /tm- d:\test\
- 10sfr56g.exe /OK- "d:\Program Files\"

Below are a few most commonly used ways of specifying path to objects which should be scanned:

- * - scan all files on all disks
- C: - scan all files on disk C
- D:\Games - scan all files in the specified folder
- C:\games* – scan all files and subfolders in the specified folder

## Command Line Parameters

**/AA** – apply actions to detected threats automatically.

**/AR** – check archive files. Option is disabled by default.

**Dr.Web CureIt!** does not scan contents of archives by default. To enable this feature, you have to specify the **/AR** command line parameter explicitly.

To check files in archives when running scan from GUI, select the **Archives** checkbox on the Excluisions tab of the **Dr.Web CureIt!** settings.

**/AC** – check installation packages. Option is disabled by default.

**Dr.Web CureIt!** does not scan installation packages by default. To enable feature, you have to specify the **/AC** command line parameter explicitly.

To check files in installation packages when running scan from GUI, select the **Installation packages** checkbox on the Excluisions tab of the **Dr.Web CureIt!** settings.

**/AFS** – use forward slash to separate paths in archive. Option is disabled by default.

**/ARC**:<*ratio*> – maximum archive object compression. If the compression rate of the archive exceed the limit, scanner neither unpacks, nor scans the archive (*unlimited*).

**/ARL**:<*level*> – maximum archive level (*unlimited*).

**/ARS**:<*size*> – maximum archive size. If the archive size exceed the limit, scanner neither unpacks, nor scans the archive (*unlimited*, KB).

**/ART**:<*size*> – minimum size of a file inside an archive beginning from which compression ratio check will be performed (*unlimited*, KB).

**/ARX**:<*size*> – maximum size of objects in archives that should be checked (*unlimited*, KB).

**/BI** – show information on **Dr.Web virus databases**. Option is enabled by default.

**/DR** – scan folders recursively (i.e., scan subfolders). Option is enabled by default.

**/E**:<*engines*> – maximum number of **Dr.Web Engines** to use.

**/FAST** – run an express scan scan of the system.

**/FL**:<*path*> – scan files listed in the specified file.

**/FM**:<*masks*> – scan files matching the specified masks. By default, all files are scanned.

**/FR**:<*regexpr*> – scan files matching the specified regular expression. By default all files are scanned.

**/FULL** – perform a full scan of all hard drives and removable data carriers (including boot sectors).

**/HA** – use heuristic analysis to detect unknown threats. Option is enabled by default.

**/LITE** – perform a basic scan of random access memory and boot sectors of all disks as well as a check on rootkits. This parameter disables the **/FAST** or **/FULL** modes.

**/LN** – resolve shell links. Option is disabled by default.

**/MA** – check email. Option is enabled by default.

**/MC**:<*limit*> – set maximum number of cure attempts to 'limit' (*unlimited*, number).

**/NB** – do not backup cured or deleted files. Option is disabled by default.

**/NI[:X]** – limits usage of system resources at scanning and priority of the scanning process (*unlimited*, %).

**/NOREBOOT** – cancel system reboot or shut down after scanning.

**/NT** – check NTFS streams. Option is enabled by default.

**/OK** – display the full list of scanned objects showing **OK** for clean files. Option is disabled by default.

**/P**:<*priority*> – priority of the current scanning task:

*0* – the lowest
*L* – low
*N* – general (used by default)
*H* – the highest
*M* – maximal

**/PAL**:<*level*> – maximum pack level (*1000*, number).

**/RA**:<*file.log*> – append the specified file with the current scanning report. By default, report is not generated.

**/RP**:<*file.log*> – rewrite the specified file with the current scanning report. By default, report is not generated.

**/QNA** – double quote file names.

**/QUIT** – terminate **Dr.Web CureIt!** once scanning completes whenever or not the detected threats are neutralized.

**/REP** – follow symbolic links while scanning. Option is disabled by default.

**/SCC** – show contents of complex objects(archives, e-mail attachments, file containers). Option is disabled by default.

**/SCN** – show names of installation packages. Option is disabled by default.

**/SPN** – show names of packers. Option is disabled by default.

**/SST** – display file scan time. Option is disabled by default.

**/TB** – check boot sectors including master boot record (MBR) of the hard drive. Option is disabled by default.

**/TM** – check processes in memory including Windows system control area. Option is disabled by default.

**/TR** – check system restore points. Option is disabled by default.

**/W**:<*time*> – maximum time to scan (*unlimited*, seconds).

**/X:S[:R]** – after scanning, shutdown, reboot, suspend, or hibernate the computer

### Settings Actions For Threats

Use the following modifiers to select an action:

- **C** – cure
- **Q** – move to quarantine
- **D** – delete
- **I** – ignore

Use the following parameters to set actions for different types of threats:

- /**AAD:**<*action*> – action for adware (possible actions: DQI).
- **/AAR:**<*action*> – action for infected archives (possible actions: DQI).
- **/ACN:**<*action*> – action for infected installation packages (possible actions: DQI).
- **/ADL:**<*action*> – action for dialers (possible actions: DQI).
- **/AHT:**<*action*> – action for hacktools (possible actions: DQI).
- **/AIC:**<*action*> – action for incurable files (possible actions: DQ).
- **/AIN:**<*action*> – action for infected files (possible actions: CDQ).
- **/AJK:**<*action*> – action for jokes (possible actions: DQI).
- **/ARW:**<*action*> – action for riskware (possible actions: DQI).
- **/ASU:**<*action*> – action for suspicious files (possible actions: DQI).

## Parameter Modifiers

Several parameters may have modifiers that clearly enable or disable options specified by these keys. For example:

- To explicitly disable scanning of installation packages, use **/AC-**
- To explicitly enable scanning of installation packages, use **/AC** or **/AC+**

These modifiers can be useful when the necessary parameter is enabled or disabled by default.

The following parameters accept these modifiers:

**/AR**, **/AC**, **/AFS**, **/BI**, **/DR**, **/HA**, **/LN**, **/MA**, **/NB**, **/NT**, **/OK**, **/QNA**, **/REP**, **/SCC**, **/SCN**, **/SPN**, **/SST**, **/TB**, **/TM**, **/TR**.

For the **/FL** parameter, the negative ('-') modifier directs to scan paths listed in the specified file and then delete this file.

For the **/ARC**, **/ARL**, **/ARS**, **/ART**, **/ARX**, **/NI[:X]**, **/PAL**, and **/W** parameters, the **0** value for the variable means that there is no limit.

If several alternative parameters are found in the command line, the last of them takes effect.

# Technical Support

Support is available to customers who have purchased a commercial version of **Dr.Web** products. Visit **Doctor Web Technical Support** website at http://support.drweb.com/.

If you encounter any issues installing or using company products, take advantage of the following **Doctor Web** support options:

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Look for the answer in Dr.Web knowledge database at http://wiki.drweb.com/
- Browse Dr.Web official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, visit the **official Doctor Web website** at http://company.drweb.com/contacts/moscow.

© 2015 Doctor Web